Annual 47 C.F.R. § 64.2009(e) CPNI Certification

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

1. Date filed: February 26, 2019

2. Name of companies covered by this certification and their Form 499 Filer IDs:

   Vyve Broadband A, LLC 829790

   Vyve Broadband J, LLC 829791

3. Name of signatory: Marie Censoplano

4. Title of signatory: General Counsel and Senior Vice President - Content Acquisition

5. Certification:

I, Marie Censoplano, certify that I am an officer of each of Vyve Broadband A, LLC and Vyve Broadband J, LLC (together, the "Company"), and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures for compliance with the CPNI rules set forth in section 64.2001 *et seq.* of the Commission's rules as described in the accompanying statement attached to this certification. See 47 C.F.R. § 64.2001 *et seq.*

The Company has not taken actions (i.e., proceedings instituted or petitions filed by the Company at either state commissions, the court system, or at the Commission) against data brokers in the past year. The Company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The Company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission. The Company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Marie Censoplano
General Counsel and Senior Vice President –
Content Acquisition
Vyve Broadband A, LLC and
Vyve Broadband J, LLC
Executed February 22, 2019

[Updated February 2019]

CPNI Compliance Policies of Vyve Broadband

The following summary describes the policies of Vyve Broadband, LLC, including its subsidiaries, Vyve Broadband A, LLC and Vyve Broadband J, LLC (together, "Vyve") that are designed to protect the confidentiality of Customer Proprietary Network Information ("CPNI") pursuant to the rules of the Federal Communications Commission ("FCC") set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq*. CPNI is "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."

Vyve's CPNI Compliance Manager manages these policies.

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

Vyve will use, disclose, or permit access to individually identifiable CPNI only in connection with its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including the publishing of directories; to initiate, render, bill and collect for communications services; to protect the rights or property of Vyve, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide inside wiring installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

Vyve does not use CPNI to market service offerings among the different categories of service, or even within the same category of service, that it provides to subscribers. Although current Vyve policy is not to use CPNI for marketing, in the event that any employee or agent wishes to use CPNI for marketing or to seek customer approval for such use, such proposed use is subject to a supervisory review process that shall involve a supervisor designated by the senior employee responsible for marketing and the CPNI Compliance Manager. If such use is approved, Vyve shall modify these policies and conduct additional training as needed to assure compliance with the FCC's rules.

Vyve does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

When Vyve receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

Above and beyond the specific FCC requirements, Vyve will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to Vyve's existing policies that would strengthen protection of CPNI, they should report such information immediately to Vyve's CPNI Compliance Manager so that Vyve may evaluate whether existing policies should be supplemented or changed.

A. Inbound Calls to Vyve Requesting CPNI

CSRs may not disclose any CPNI to an inbound caller until the caller's identity has been authenticated using methods appropriate for the information sought prior to revealing any CPNI or account information to the inbound caller.

More stringent protections apply to Call Detail Information (CDI), which includes any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call. Even after a caller has been authenticated under the process above, a CSR will not reveal Call Detail Information (CDI) to an inbound caller.

Instead, if an inbound caller requests CDI, the information will be sent to an address of record for the account, but only if such address has been on file with Vyve for at least 30 days. In the event that a customer has changed his or her address within the prior 30 days, or if the customer advises that they no longer have access to mail sent to that address, the information will be made available to the customer at a company office after being authenticated in accordance with subsection B below.

B. In-Person Disclosure of CPNI at Vyve Offices

Vyve may disclose a customer's CPNI to an authorized person visiting a Vyve office upon verifying that person's identity through a valid, non-expired government-issued photo ID (such as a driver's license, passport, or comparable ID) matching the customer's account information.

C. Online Accounts

To access an online account from which a customer can access their CPNI, a customer must enter a PIN and create a password. The PIN is randomly generated by Vyve at the time of service installation, provided to the customer's address of record, or provided to the customer in a Vyve office after being authenticated in accordance with the requirements for in-person CPNI disclosure.

D. Notice of Account Changes

Whenever a PIN, password or online account is created or changed, Vyve is required to provide a notice to the customer's address of record. Whenever an address of record is created or changed, Vyve sends a notice to customer's prior address of record notifying them of the change. The foregoing notifications are not required when the customer initiates service, including the selection of an email address or creation of an online account at service initiation. Each of the notices provided under this subsection will not reveal the changed information and will direct the customer to notify Vyve if they did not authorize the change.

E. Business Customer Exemption

The authentication requirements for disclosure of CPNI set forth in this Section II do not apply to business customers that have a dedicated account representative and that have a contract with Vyve that specifically addresses the protection of CPNI.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Any Vyve employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to Vyve's CPNI Compliance Manager. Such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is Vyve's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to our customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate Vyve's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

A. Identifying a "Breach"

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Manager.

If a Vyve employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to Vyve's CPNI Compliance Manager who will determine whether to report the incident to law enforcement and/or take other appropriate action. Vyve's CPNI Compliance Manager will determine whether it is appropriate to update Vyve's CPNI policies or training materials in light of any new information. The FCC's rules require Vyve on an ongoing basis to

"take reasonable measures to discover and protect against activity that is indicative of pretexting."

B. Notification Procedures

As soon as practicable, and in no event later than seven (7) business days upon learning of a breach, the CPNI Compliance Manager shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: https://www.cpnireporting.gov. Vyve's FRN number and password may be required to submit a report. If this link is not responsive, the CPNI Compliance Manager should contact counsel or the FCC's Enforcement Bureau (202-418-7450) for instructions.

Vyve will not notify customers or disclose a breach to the public until seven (7) full business days have passed after notification to the USSS and the FBI except as provided below. (The business day on which the notice was provided will not be counted as a full business day.) Federal law requires compliance with this requirement even if state law requires disclosure. If Vyve receives no response from law enforcement after the 7th full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

Vyve will delay notification to customers or the public upon request of the FBI or USSS. If the CPNI Compliance Manager believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; Vyve still may not notify customers sooner unless given clearance to do so from *both* the USSS and the FBI.

IV. RECORD RETENTION

Vyve's CPNI Compliance Manager is responsible for assuring that we maintain for at least two (2) years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Vyve maintains a record, for a period of at least one (1) year, of those limited circumstances in which CPNI is disclosed or provided to third parties or where third parties were allowed access to CPNI. If Vyve later changes its policies to permit the use of CPNI for marketing, it will revise its recordkeeping policies to comply with the Commission's recordkeeping requirements.

Vyve maintains a record of all customer complaints related to their handling of CPNI, and records of Vyve's handling of such complaints, for at least two (2) years. The CPNI Compliance Manager will assure that all complaints are reviewed and that Vyve considers any necessary changes to its policies or practices to address the concerns raised by such complaints. An authorized corporate officer will sign a compliance certificate on an annual basis stating that the officer has personal knowledge that Vyve has established operating procedures that are adequate to ensure compliance with FCC's CPNI rules. The certificate for each year will be filed with the

FCC by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how Vyve's operating procedures ensure compliance with the FCC's CPNI rules. In addition, the filing must include an explanation of any actions taken against data brokers and a summary of any customer complaints received in the past year concerning the unauthorized release of CPNI. Confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

V. TRAINING

All employees with access to CPNI receive a copy of Vyve's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, Vyve requires CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, and marketing personnel.